AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method of enabling a lookups between connected devices, the method comprising:

generating one or more cryptographic keys associated with a namespace;

creating an authority using one of the cryptographic keys;

enabling one or more namespaces to refer to the authority via requesting authorities associated with the one or more namespaces to issue a peer-to-peer type resolution so that names of the namespaces resolve to the authority; and

for any other namespaces to which communication is desired, issuing a resolution that names the authority and one or more names associated with the other namespaces to resolve to one or more of the other authorities.

2. (Original) The method of claim 1 wherein the connected devices are part of a peer-to-peer network cloud.

3. (Original) The method of claim 1 wherein the peer-to-peer type resolution means that for one or more namespaces S_1, S_2, ... S_N with names N_1, N_2, ...N_N for which communication and referencing is desired a request to authorities is made for the namespaces to issue $([S_1].N_1) \rightarrow A$, $([S_2].N_2) \rightarrow A$, ... $([S_N].N_N) \rightarrow A$ so that the names N_1, N_2, ... N_N resolve to the authority.

4. (Original) The method of claim 1, further comprising: for any services, publishing the authority and a service name to receive an end result that provides data.

5. (Original) The method of claim 1, further comprising: for any services, publishing the authority and a service name to receive an IP address, a protocol name and a port.

6. (Original) The method of claim 1 further comprising: dynamically changing one or more addresses associated with the authority via delegating the authority to another name associated with one or more added addresses.

7. (Currently amended) The method of claim 1 wherein the lookup resolves to one of the group arbitrary data, hosts and services.

8. (Original) The method of claim 1 wherein creating the authority includes performing a hash of the cryptographic key, the cryptographic key being a public key from a private key-public key pair.

9-18 (Canceled)

19. (Currently amended) A method of generating a data structure for implementing a name resolution protocol, ~~the data structure~~ comprising:

generating a first field comprising an authority component associated with a public key, the public key being part of a private key-public key pair; and

generating a second field comprising a name component associated with a namespace of an ~~the~~ owner of the private key-public key pair, wherein the authority component and the name component are capable of resolving to a second authority or to an address of a machine.

20. (Currently amended) The ~~data structure~~ method of claim 19, wherein the authority component and the name component are capable of resolving to a port number, a protocol name, and an IP address.

21. (Currently amended) The ~~data structure~~ method of claim 19, wherein the authority component and the name component are capable of resolving to arbitrary data.

22. (Currently amended) The ~~data structure~~ method of claim 19 ~~wherein one or more of an IP address, protocol name and port can be retrieved from a cache~~, further comprising retrieving one or more from the group an IP address, a protocol name, and a port number from a cache.

23. (Currently amended) A computer readable medium ~~having stored therein instructions~~ tangibly embodying a program of instruction executable by a computer for performing ~~acts~~ steps for enabling a lookup ~~lookups~~ between connected devices, the ~~acts~~ steps comprising:

generating one of more cryptographic keys associated with a namespace;

creating an authority using one of the cryptographic keys;

enabling one or more namespaces to refer to the authority via requesting authorities associated with the one or more namespaces to issue a peer-to-peer type resolution so that names of the namespaces resolve to the authority; and

for any other namespaces to which communication is desired, issuing a resolution that names the authority and one or more names associated with the other namespaces to resolve to one or more of the other authorities.

24. (Original) The computer readable medium of claim 23 wherein the connected devices are part of a peer-to-peer network cloud.

25. (Original) The computer readable medium of claim 23 wherein the peer-to-peer type resolution means that for one or more namespaces S_1, S_2, ... S_N with names N_1, N_2, ...N_N for which communication and referencing is desired a request to authorities is made for the namespaces to issue $([S_1].N_1) \rightarrow A$, $([S_2].N_2) \rightarrow A$, ... $([S_N].N_N) \rightarrow A$ so that the names N_1, N_2, ... N_N resolve to the authority.

26. (Currently amended) The computer readable medium of claim 23 wherein the steps ~~acts~~ further comprise: for any services, publishing the authority and a service name to receive one or more of arbitrary data, an IP address, a protocol name and a port.

27. (Currently amended) he computer readable medium of claim 23 wherein the steps ~~acts~~ further comprise: dynamically changing one or more addresses associated with the authority via delegating the authority to another name associated with one or more added addresses.

28. (Original) The computer readable medium of claim 23 wherein the lookup resolves to hosts and services.

29. (Original) The computer readable medium of claim 23 wherein the lookup resolves to arbitrary data.

30. (Currently amended) The computer readable medium of claim 23 wherein creating the authority ~~includes~~ comprises performing a hash of the cryptographic key, the cryptographic key being a public key from a private key-public key pair.

31-38 (Canceled)